



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

AERONAUTICAL INFORMATION SYSTEM SECURITY (AISS) FRAMEWORK GUIDANCE

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-201

December 2015

102 rue Etienne Dolet
92240 MALAKOFF, France
Web Site: www.eurocae.net

 Tel: 33 1 46 55 62 65
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net
Document Sharing Hub

AERONAUTICAL INFORMATION SYSTEM SECURITY (AISS) FRAMEWORK GUIDANCE

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ED-201

December 2015

© EUROCAE, 2015

 **Documents**
Document Sharing Hub

FOREWORD

1. This document was prepared by EUROCAE Working Group 72 "Aeronautical Systems Security", and was approved by the Council of EUROCAE on 25 December 2015.
2. EUROCAE is an international non-profit making organisation in Europe. Membership is open to manufacturers and users of equipment for aeronautics, trade associations, national civil aviation administrations, and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. The findings of EUROCAE are resolved after discussion amongst Members of EUROCAE and in collaboration with RTCA Inc, Washington D.C., and/or the Society of Automotive Engineers (SAE), Warrendale PA, U.S.A., through their appropriate committees.
4. EUROCAE performance specifications and other documents are recommendations only. EUROCAE is not an official body of the European Governments. Its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
5. Copies of this document may be obtained from:

EUROCAE
102, rue Etienne Dolet
92240 MALAKOFF
France

Telephone: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net
Website: www.eurocae.net

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	1
1.1 PURPOSE AND SCOPE	1
1.2 ED-201 – AERONAUTICAL INFORMATION SYSTEM SECURITY FRAMEWORK GUIDANCE	2
1.3 ED-202A – AIRWORTHINESS SECURITY PROCESS SPECIFICATION	3
1.4 ED-203 – AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS	3
1.5 ED-204 – INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS	4
1.6 HOW TO USE ED-201	4
CHAPTER 2 CONSIDERATIONS OVERVIEW	6
2.1 PRINCIPLES	6
2.2 EXTERNAL AGREEMENTS	6
2.3 A CIVIL AVIATION STAKEHOLDER FRAMEWORK	7
2.4 RISK MANAGEMENT APPROACH	9
2.4.1 The international context for risk assessment and risk management	10
2.4.2 Risk Management Methods	12
2.4.3 Acceptable Risk Levels	13
2.4.4 Types of risk	14
2.5 SECURITY ENVIRONMENT	15
2.6 THE EFFECT OF CHANGES OVER TIME	16
2.6.1 Product Life-cycle	16
2.6.2 Transition between Life-cycle Phases	17
2.6.3 Evolution of Technology and Attacks	19
2.6.4 Threat Source Changes	20
2.6.5 Needs and challenges of security updates and changes	20
2.7 SHARING SECURITY-RELATED INFORMATION	21
2.7.1 Incidents	22
2.7.2 Vulnerabilities	22
2.7.3 Threats	22
2.7.4 Assessments of shared risks	23
2.7.5 Risk treatment plans	23
2.7.6 Security assurance activities	23
2.8 ASSURANCE OF INFORMATION SECURITY	23
2.9 IDENTIFYING AND MITIGATING SHARED RISK	24
2.9.1 Shared Responsibilities	25
2.9.2 The Need for Assessments of Shared Risks	25
2.9.3 The need for Multilateral External Agreements	26

CHAPTER 3 INTER-ORGANISATIONAL NEEDS	28
3.1 SECURITY MANAGEMENT SYSTEMS AND RISK MANAGEMENT REQUIREMENTS	28
3.2 COMPARABILITY OF RISK ASSESSMENTS	29
3.2.1 Comparability requirements	29
3.2.2 Risk assessment template	29
3.3 SHARING INCIDENT AND VULNERABILITY INFORMATION	34
3.3.1 Introduction	34
3.3.2 Sharing from the perspective of an operational organisation	35
3.3.3 Sharing from the perspective of the product developer:	37
3.3.4 Government activities in incident and vulnerability sharing	39
3.3.5 Recommendations for sharing incident and vulnerability information	40
3.4 ASSURANCE	40
3.4.1 Assurance methods	40
3.4.2 Effectiveness and correctness	42
3.5 EXTERNAL AGREEMENTS FOR SECURITY	42
3.5.1 Requirements for a multi-lateral agreement template	42
3.5.2 External Agreement components	43
APPENDIX A: COMPARING THE ISO 27005 FRAMEWORK, ICAO RCS AND NIST PROCESS	45
APPENDIX B: ED-201 GLOSSARY	48
APPENDIX C: REFERENCES	50
APPENDIX D WG-72 MEMBERSHIP	52
IMPROVEMENT SUGGESTION FORM	55

LIST OF FIGURES

Figure 1: RELATIONSHIPS BETWEEN STAKEHOLDERS	9
Figure 2: TYPES OF RISK	9
Figure 3: RELATIONSHIP OF LIFE-CYCLE PHASES OF SEPARATE PRODUCTS.....	18
Figure 4: IMPACT AND REQUIRED ATTACK CAPABILITY OVER TIME	21
Figure 5: THREAT INFORMATION CATEGORIES	23
Figure 6: MULTI-LEVEL ORGANISATION-SIDE RISK MANAGEMENT (FROM NIST SP800-39)	28
Figure 7: RISK ASSESSMENT STAGES.....	29
Figure 8: SOME STANDARD STEPS IN AN INCIDENT RESPONSE PROCESS	35
Figure 9: STAKEHOLDERS FOR AN OPERATIONAL ORGANISATION	36
Figure 10: STAKEHOLDERS FOR A DEVELOPMENT ORGANISATION	38
Figure 11: ASSURANCE IN DEVELOPMENT LIFECYCLE STAGES.....	42
Figure 12: ICAO RISK CONTEXT STATEMENT (RCS) METHOD	45
Figure 13: COMPARISON BETWEEN ICAO RCS AND ISO27005 METHODS	46
Figure 14: COMPARISON BETWEEN NIST AND ISO27005 METHODS	47

CHAPTER 1

INTRODUCTION

1.1 PURPOSE AND SCOPE

This document is concerned with the overarching context of the shared responsibility for Aeronautical Information Systems Security (AISS) through the identification and description of topics which have to be addressed. This responsibility is shared by all relevant stakeholders who are part of civil aviation. The purpose of security in this context shall be understood as ensuring safety of flight, and maintaining the operation of the civil aviation infrastructure without significant disruption.

It covers all areas of Civil Aviation relevant to this purpose, including aircraft design, production and operation (passenger and cargo), air traffic management, airports, maintenance repair and overhaul operations (MRO), aviation service providers, components (such as avionics hardware and software, databases, configuration data, etc.) and information (such as NOTAMS, weather, obstacles, routes & restrictions, manuals & charts, etc.) and the supply chains which these use and comprise.

Some of the concepts covered in this guidance relate to what should be done in civil aviation rather than to current practice. Since the concepts need to be implemented by partners across the civil aviation sector their adoption will initially be piecemeal, and the full benefit will not be achieved until a critical mass of stakeholders have adopted them. Early adopters will therefore need to bear this in mind, but they will be achieving increasing levels of benefit as the concepts are adopted. Also the extent to which the concepts are applicable will vary across civil aviation. For example some of them will have limited applicability to business and general aviation.

This document also provides an introduction to all documents related to Aeronautical Information Systems Security (AISS) published by EUROCAE, which are (at the time of publication):

- ED-201 Aeronautical Information System Security Framework Guidance
- ED-202A Airworthiness Security Process Specification
- ED-203 Airworthiness Security Methods and Considerations
- ED-204 Information Security Guidance for Continuing Airworthiness

In addition to these EDs, a Glossary will be published as a EUROCAE report, to serve as the centralized and normative Definition of Terms, shared by all EUROCAE documents addressing Aeronautical Information Systems Security. However, the published documents do not cover all aspects of AISS. EUROCAE may develop additional documents for other AISS aspects in the future. Identified potential topics include CNS/ATM security and supply chain security.

RTCA Inc. has published DO-326A, which has the same technical contents as ED-202A, and DO-355 has the same technical contents as ED-204.

This document describes a framework for information system security¹ for civil aviation (AISS), based on certain underlying principles:

- that information security exists to minimise occurrences and impacts of intentional unauthorised electronic interaction with information and communication systems;
- that the security objectives are derived from both safety objectives and from the need to minimise disruption to the air traffic system;
- that the International Civil Aviation Organization (ICAO) has already established that “measures... to protect information and communication technology ... from interference” are required², and that the ICAO Member States have agreed to this;
- that States can require the organisations comprising civil aviation in their own territory to meet these requirements;
- that civil aviation depends on co-operation and collaboration between all suppliers, manufacturers, operators and service providers, and that this applies strongly to security;
- that co-operative and collaborative information security is more effective and efficient than independent and isolated information security.

1.2

ED-201 – AERONAUTICAL INFORMATION SYSTEM SECURITY FRAMEWORK GUIDANCE

There are many standards and guidance documents which address the responsibility that each organisation has for its own information security, dealing with internal systems, processes, products and data. However this guidance looks beyond the individual organisation at information security related to systems and processes, and to products and data, in a wider context. This guidance concentrates on the shared information risk which is inherent in the situation where systems, processes, products or data are shared, or are passed from one organisation to another. There are varying degrees of sharing and exchange in these situations but any sharing or exchange causes additional risk to an organisation. This guidance is most applicable to the larger risks, which affect safety or where there are significant implications for service delivery. Smaller risks (assuming they have been correctly assessed) require less effort particularly in mitigations and this guidance should be interpreted accordingly.

The foundation for AISS is the concept of a standardised External Agreement which covers the information security issues around an external interface and/or use of third-party products. The External Agreement concept requires sharing information security information about the interface or product, which is also covered in this guidance. This approach is based on managing the shared risk which are created by the interface or product use. The risk is the direct result of using 3rd party products, linking networks and/or sharing data. It has some similarities to what is often referred to as “supply-chain risk”, but this guidance goes further, and deals with multilateral relationships rather than just the bi-lateral ones which characterise a simple supply chain.

¹ Also often referred to as cyber security. The differences between information security and cyber security are not so great as to cause a problem in this guidance, so the differences are therefore ignored;

² ICAO Convention (Doc 7300) Annex 17, 9th edition, Section 4.9

1.3

ED-202A – AIRWORTHINESS SECURITY PROCESS SPECIFICATION

The guidance in ED-202A adds to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and is intended to be used in conjunction with other applicable guidance material, including ED-79A / SAE ARP4754A, ED-135 / SAE ARP4761, ED-12C / DO-178C, and ED-80 / DO-254 and with the advisory material associated with FAA AC 25.1309 and EASA AMC25.1309, in the context of Part 25 and CS-25. Tailoring of this guidance may allow it to be applicable in other contexts such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33.

ED-202A guidance material is for equipment manufacturers, aircraft manufacturers, and anyone else who is applying for an initial Type Certificate (TC), and afterwards (e.g. for Design Approval Holders (DAH)), Supplemental Type Certificate (STC), Amended Type Certificate (ATC) or changes to Type Certification for installation and continued airworthiness for aircraft systems, and is derived from understood best practice.

Special caution is recommended when applying the guidance to developments or operations already in place. The guidance is designed to be implemented across the full life cycle of an aircraft from design, through operations, to disposal. As such, it should first be applied to the design stage before its use in subsequent stages of the life cycle. If objectives are applied to aircraft which were not previously subject to these objectives during all stages of its life cycle, then it should be borne in mind that some aspects of the objectives will not be applicable. These aspects should be described and dealt with separately. For existing aircraft or aircraft in development, alternate processes are acceptable which may utilize some or all of the processes in ED-202A.

Compliance may be accomplished through differentiated but interacting processes for security and safety. To sustain this approach, overall consistency between both processes should be maintained, by ensuring that the security process considers the outputs of the safety assessment process. As an alternative, when considered practicable, compliance may be accomplished through a blended process – documented by the applicant – that would integrate safety and security, including suitable evidences that security and safety requirements are met.

1.4

ED-203 – AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

This document provides guidance on a set of methods and guidelines for applicants implementing an Airworthiness Security Process as specified in ED-202A / DO-326A to address information security for certification of aircraft and its systems. More specifically, it addresses the activities in the areas of security risk management and security assurance. Applicants and authorities should consider these methods, and alternative practices if and when they are proposed. Those aspects of information security that have no safety effect are not in the scope of ED-203.

Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction. Intentional unauthorized electronic interaction (also known as "unauthorized interaction" within the scope of ED-203) is defined as human-initiated actions with the potential to affect the aircraft due to unauthorized access, use, disclosure, denial, disruption, modification, or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effects of malware on infected devices and the logical effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming.

The guidance provides methods and considerations for securing airworthiness during the aircraft life cycle. It was developed as a companion document to ED-202A / DO-326A "Airworthiness Security Process Specification" which addresses security aspects of aircraft certification and ED-204 / DO-355 "Information Security Guidance for Continuing Airworthiness" which addresses airworthiness security for continued airworthiness.

ED-203 assumes knowledge of other applicable guidance material, including e.g. ED-79A / ARP 4754A, ED-135 / ARP 4761, ED-12C / DO-178C, and ED-80 / DO-254 and with the advisory material associated with FAA AC 25.1309 and EASA AMC 25.1309, in the context of Part 25 and CS-25. Tailoring of this guidance may allow it to be applicable in other contexts such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33.

1.5 ED-204 – INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

This document provides guidance for the operation and maintenance of aircraft and for organisations and personnel involved in these tasks. It shall support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and the responsibilities of aircraft operators to maintain their aircraft, to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels. As all information security threats may have an intentional origin, ED-204 also covers electronic sabotage (as used in AMC 25.1309).

ED-204 is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

ED-204 also gives guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects). Thus, it also supports harmonizing security guidance documents among Design Approval Holders (DAH), which is deemed beneficial to DAHs, operators and civil aviation authorities. The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, ED-204 does not make any assumptions about and is without prejudice to its applicability.

1.6 HOW TO USE ED-201

The fundamental organisational process being put forward in this guidance has two aspects:

1. Address internal security:
 - a. Implement standards (NIST, ISO or other as appropriate) or use a standards-based approach
 - b. Establish an Information Security Management System (ISMS) incorporating a risk management approach, as part of a Security Management System (SeMS)
 - c. Establish monitoring and change control processes to ensure any system changes are correct and authorised
 - d. Establish processes to measure assurance for the ISMS
2. Address external security:
 - a. Identify partners through external interfaces and inputs/outputs, including network connections, 3rd party products and information exchanges
 - b. Risk-assess these interfaces/products and share the results with the partners
 - c. Obtain the partners' risk assessment information for the same interfaces and inputs/outputs
 - d. Modify internal practices based on the shared information
 - e. Repeat until each supply chain or information flow is fully assessed

This approach means that at each interface between organisations the following questions need to be answered:

- Do the partners agree that the shared risks have been properly identified and assessed?
 - this includes apportioning the shared risk between the organisations
- Do the partners agree that effective mitigations are in place?
 - These may be mitigations in place in either organisation or in a third-party with which either organisation has an agreement
- Do the partners agree that the mitigations are working adequately and as expected?

The information that provides the answers to the questions above will come partly from participation in shared processes, (particularly vulnerability management, and incident response and management), and partly from sharing the results of separate but compatible processes, such as risk management, and security protection effectiveness assessment.

The information that provides the answers to these questions will be embodied in an External Agreement between the organisations concerned. The External Agreement is a result of the Risk Management process, as applied to an organisation's external interfaces. It embodies the results of the risk assessment and risk treatment plans and acts as the means of communicating with external organisations. By standardising both the requirement for this External Agreement and its contents, it will be possible to secure multi-party interfaces and information flows which include a number of organisations.

Section 2 of this guidance discusses why activities are necessary. Section 3 describes the necessary activities and their inputs and outputs. Readers familiar with the concepts of multilateral risk assessment and management, the aviation security environment and information security assurance, will be able to go straight to Section 3.

CHAPTER 2

CONSIDERATIONS OVERVIEW

2.1 PRINCIPLES

The following principles are examined further in the following subsections:

- External Agreements express the trust placed in an external interface.
- Security activities should be done in the most efficient place, but are subject to stakeholder agreement.
- Risk Management enables assessment and evaluation of risks internally and their description in External Agreements.
- Security activities (and attacks) take place in a Security Environment which extends beyond an individual system and across partners.
- The Security Environment changes over time so there will need to be changes to both the risk assessment and the risk treatments described in the External Agreements.
- Organisations must assure security activities against the requirements identified in the risk assessment.
- Information on internal assessments, actions and assurance must be shared with partners to the extent required to secure the interface effectively.

2.2 EXTERNAL AGREEMENTS

The External Agreement addresses the fundamental information security problem caused by using 3rd party products, linking networks and sharing data, which comes down to a question of trust. Trust is a fundamental quality in business relationships and trust as a concept is applicable to both organisations and individual information systems. As it is expressed in NIST SP800-39³:

“Organisations are becoming increasingly reliant on information system services and information provided by external organisations as well as partnerships to accomplish missions and business functions. This reliance results in the need for trust relationships among organisations. In many cases, trust relationships with external organisations, while generating greater productivity and cost efficiencies, can also bring greater risk to organisations. This risk is addressed by the risk management strategies established by organisations that take into account the strategic goals and objectives of organisations.”...

“Two factors affecting the trustworthiness of information systems are:

- *Security functionality (i.e., the security features/functions employed within the system); and*
- *Security assurance (i.e., the grounds for confidence that the security functionality is effective in its application).*

Security functionality can be obtained by employing ... a combination of management, operational and technical security controls ...

³ NIST SP800-39, Managing Information Security Risk: Organization, Mission, and Information System View, Mar 2011

Security assurance is a critical aspect in determining the trustworthiness of information systems. Assurance is the measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. Assurance is obtained by:

- *the actions taken by developers and implementers with regard to the design, development, implementation, and operation of the security functionality (i.e., security controls); and*
- *the actions taken by assessors to determine the extent to which the functionality is implemented correctly, operating as intended, and producing the desired respect to meeting the security requirements for information systems and their environments of operation.”⁴*

The requirements for establishing, assessing and assuring information security functionality for aircraft are also dealt with in more detail in ED-202A, ED-203 and ED-204. Security assurance is also considered in more detail in section 3.4 of this guidance.

2.3

A CIVIL AVIATION STAKEHOLDER FRAMEWORK

In security, as for safety, it is important to guarantee that manufacturers, operators, maintainers, product suppliers and all service providers, put the appropriate level of investment into information security and do not create an unfair economic situation for other stakeholders. For example the level of commitment to information security of an aircraft supplemental type certification holder may be affected by a wish to save money and an assumption that someone else will pay for any necessary security. This situation requires the definition of a minimum regulatory package that would help guarantee that stakeholders are competing fairly and that the competition does not sacrifice safety.

Although the notion of a “level playing field” originally comes from the global economic competition context, it should also be applied in the aviation safety context⁵.

It may be that a protection against a risk can best be implemented by a particular organisation but the benefit will mainly be felt by other organisations. Agreement on this may be difficult to achieve, but will be more effective from the perspective of the entire civil aviation network. See Section 2.9 for more details.

However different stakeholders have different roles and thus different motivation, strengths, abilities, constraints, etc. and these differences have to be properly accounted for at the interfaces between the organisations. Stakeholders identified in this document are:

- **Manufacturers** of Aircraft, Control Centres and Systems (further referred to as “system”).
- **Operators** of Aircraft, Control Centres and Systems: Airlines, Air Navigation Service Providers (ANSPs), Airports, etc.
- **Maintainers** of Aircraft, Control Centres and Systems: (Maintenance and Repair Organisations (MROs), Airlines, Airports, etc.
- **Product Suppliers** whose products are integrated into aircraft and systems, including avionics, Electronic Flight Bags (EFBs), Notices to Airmen (NOTAMs), Navigation /Obstacle databases, etc.
- **Service Providers:** Air Navigation, Communication, Passenger & Cargo Handling, NOTAMs, etc.

⁴ NIST SP800-39 Managing Information Security Risk

⁵ For example the main objective of the EASA Basic Regulation (EC) No 216/2008 is to “establish and maintain a high uniform level of civil aviation safety in Europe” [Article 2 (1)]. One additional objective among others is “to provide a level playing field for all actors in the internal aviation market” [Article 2 (2)]. One of the means to attain such objectives is “the preparation, adoption and uniform application of all necessary acts” [Article 2 (3) (a)].

- **Governance Bodies:** Legislators, Regulators, Auditors, etc.
- **Standards Bodies:** Industry, Treaty organisations.

It is worth noting that some organisations fall into more than one category.

Manufacturers: This stakeholder group has a fundamental influence upon the security posture of a “system”. Their security decisions determine not only their own design but also strongly influence the options and obligations of other stakeholders. In doing so they are overseen – and often obliged to meet laws and regulations – by the Governance group of stakeholders. They should base their work on the standards and guidance coming from the Standards and Governance bodies.

Operators: This stakeholder group is primarily responsible for the safe and secure use of the “system” delivered. It receives related guidance from the manufacturers in doing so, while legislators provide the legal framework in which the systems can be used. Operators are generally at the receiving end of the supply chain, interfacing with the general public. They should base their work on the standards and guidance coming from the Standards and Governance bodies.

Maintainers: Maintainers support operators in keeping the equipment at a predefined and legally approved state, fit for safe and secure operation, according to instructions by the manufacturers and under supervision of the Governance stakeholders. They should base their work on the standards and guidance coming from the Standards and Governance bodies.

Service Providers: In the context addressed they mainly provide services to operators. They are linked to them through contractual relationships and regulations. They should base their work on the standards and guidance coming from the Standards and Governance bodies.

Product Suppliers: This rather diverse group of stakeholders consists of manufacturers of items of software, hardware and information, and system integrators. They are linked to other stakeholders through contractual relationships and regulations. They should base their work on the standards and guidance coming from the Standards and Governance bodies.

Governance Bodies: They are driven by the need to ensure safety and to enable an efficient and interoperable civil aviation system. The main objective is the safety of the systems under consideration, operating in a pre-determined environment. This task has been driven largely by societal acceptance and political directions, internationally coordinated through treaties and descending legislation. Security is increasingly regarded as a contributing factor to aviation safety. Critical service resilience is another increasingly important regulatory element, involving different national or regional authorities:

- International treaty organisations, e.g. the International Civil Aviation Organization (ICAO), Eurocontrol.
- National Legislators.
- Supervisory authorities (e.g. CAAs).

Standards Bodies: This group provides standards and guidance about security practices which may be adopted by Governance stakeholders. The other stakeholders contribute to the development of the standards and guidance, based on industry experience and best practice.

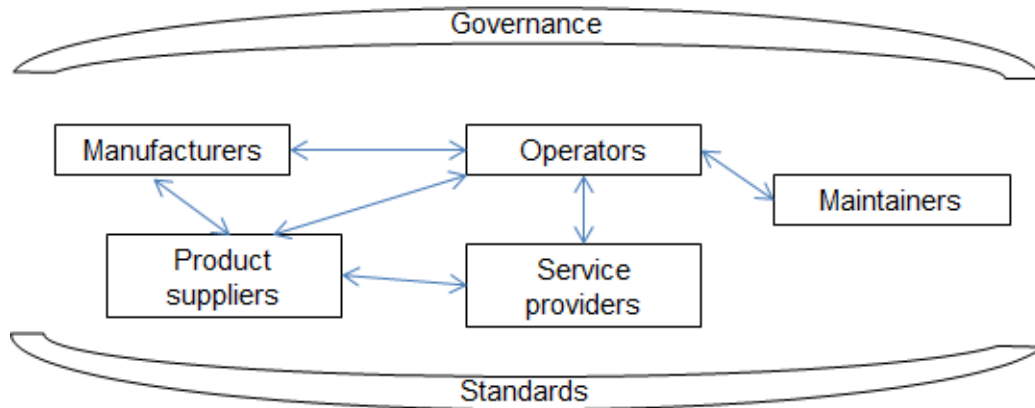


FIGURE 1: RELATIONSHIPS BETWEEN STAKEHOLDERS

2.4

RISK MANAGEMENT APPROACH

There are a number of different perspectives on Risk Management and – associated to those – Risk Assessment. Most organisations are probably using them in parallel for different purposes, not necessarily though by the same organisational units. They can be divided into a few assessments types (rule based, judgement based or probabilistic) covering a number of different classes of objectives (compliance, protection, strategy, cost or operation).

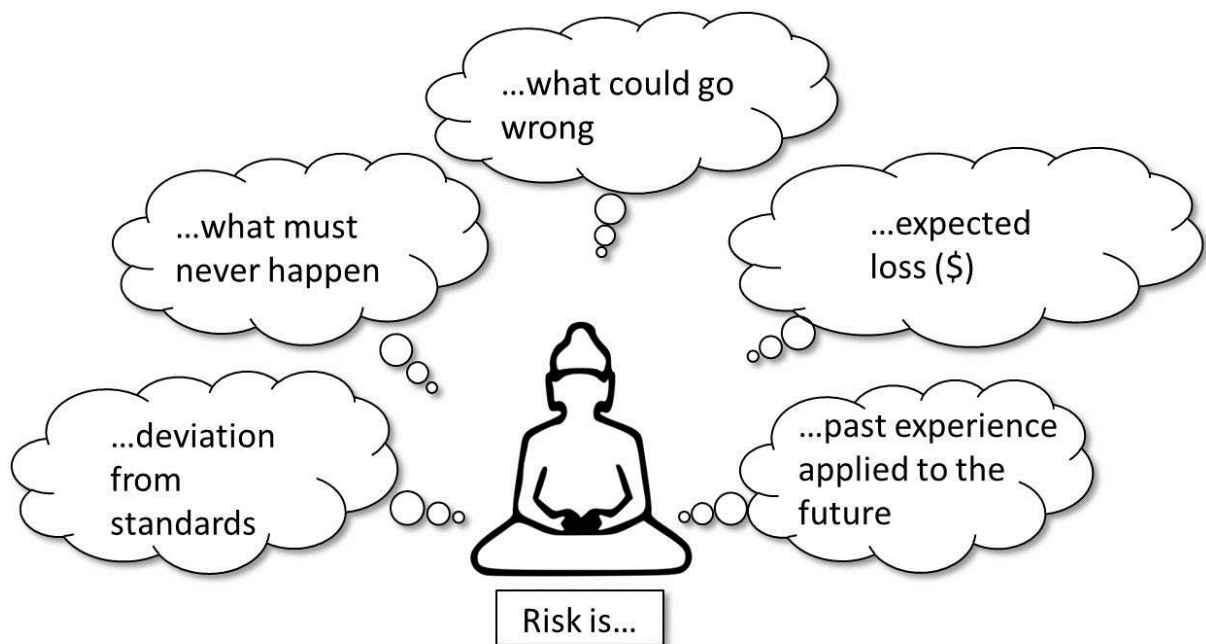


FIGURE 2: TYPES OF RISK

An aircraft example provides some rationale as to why one assessment type along with its associated risk management does not necessarily fit all applicable purposes.

Traditional safety assessments identify potential effects on aircraft caused by (development) errors and (system or item) failures. As failures are coincidentally happening their occurrences are following statistical models. Thus probabilistic risk assessment types can be applied to determine whether or not they meet certification requirements. In contrast security assessments deal with intentional acts, which are not following any statistical model. Even with longer term in-service observations it will not be possible to confirm predictions with a margin of error small enough to achieve the levels of confidence required. Thus direct calculation of probabilistic risk assessments types will not provide adequate results. Rather, protection-focused assessments types are better suited to make the determination whether or not certification requirements have been met.

In aircraft development there is a tension between safety-driven and security-driven architectures. In principle safety and security functionality must not conflict and should be reinforcing each other. During development architectures can be designed to be primarily safe or secure. During all aircraft development life-cycle phases safety has been determined to be the driving property, expressed in the Type Certification requirements. Safety and security processes should interface at multiple points to avoid unnecessary duplication, to ensure there are no gaps and to resolve all potential conflicts which may have been discovered. However, these interfaces need to be fully understood and accepted within both processes. ED-202A describes such a process for dealing with the airworthiness aspects of security.

In the development of ground-based systems the tension with safety requirements is less of an issue, but the inclusion of security risk into other existing risk management processes is still an issue. This also applies to risk management in an operational context.

While risk is an omnipresent phenomenon, risk management seeks to address significant relevant risks, and to group them into manageable units. Subsequent sections address multiple options used to assess and manage risks.

2.4.1

The international context for risk assessment and risk management

Risk management and risk assessment are terms used to cover a wide variety of different and detailed activities, although they all share the core purpose of understanding the risks to something to ensure that risk is acceptable. Acceptability can be achieved by avoiding the risky activity, by transferring the risk to others (if applicable), or by implementing security measures to mitigate the risk. In this case the something under consideration is the security of civil aviation.

Aviation security measures are set at international level through ICAO convention annexes and Standards and Recommended Practices (SARPS)⁶, and at national level⁷ in the “National Civil Aviation Security Programme” (NCASP). At the organisation level they are best devised and operated through a Security Management System (SeMS) using a formal risk-based approach. Effective aviation security also depends on the collaborative efforts of all stakeholders, which are co-ordinated so there are no exploitable gaps. As an additional benefit effective co-ordination will ensure that costs due to unnecessary overlaps are avoided.

The security measures are chosen and implemented based on the perceived risks in a risk management process. The process by which identified risks are managed is a continuous multi-activity process. Risk management as a whole comprises:

- Risk assessment, which includes describing the scope of the assessment, identifying the assets to be protected and the threats to these assets, and evaluating whether the risks are acceptable;
- Risk treatment, which is the programme of activities designed to reduce or eliminate the risks;

⁶ There may also be regional requirements, such as ECAC Doc30 in Europe

⁷ The EU also operates at the National level, in place of individual States for some functions

- Monitoring of risks, to ensure they remain at acceptable levels within an evolving security environment;
- A risk communications programme which reaches out to stakeholders and partners to share risk information.

Risk assessment is the core activity. Assessment can (and should) be done repeatedly, at different scales with relevant types of threat. Assessed threats with a sufficiently high impact and likelihood⁸ will be treated to reduce the risk to be acceptable, as part of a risk treatment or mitigation programme. Establishing what is acceptable is a significant part of the risk management process as it will determine the security measures which need to be implemented. It must be set to be compatible with the risks identified by partners and stakeholders, to ensure there are no gaps in overall aviation security. This includes the risks identified globally (by ICAO), regionally⁹ and at national level¹⁰. This is discussed in more detail later.

It should be noted that risk assessment is used as a basic tool at the international, national and organisational levels, but there are differences in usage between the levels. Clearly risks to the global civil aviation system are different to risks to national security and service continuity, which are different to the risks facing individual organisations.

In many cases these different risks have common factors, such as the threat sources and vectors and attack targets, although the assessment of the impact and likelihood of the risks will vary. Therefore risk management and assessment at the different levels can still be linked effectively, as long as the differences are understood and taken into account.

- ICAO: The ICAO Working Group on Threat and Risk uses the processes described in the Risk Context Statement (RCS) to assess broad global threat issues affecting aviation security (i.e. the result of malicious acts and not accidents, which may result in disruption and/or destruction) to provide advice to Member States¹¹.
- ICAO Member States use the output from the RCS as part of their national risk assessments as well as using their own domestic risk assessment procedures. Member States have the responsibility to ensure that organisations (both publically and privately owned) have a risk management process that includes information security risks and which takes account of national risk assessment outputs. Most attention should be paid to organisations providing critical aviation services at the national or international levels.
- Organisations will use many sources to inform their own risk management process including threats to safety, finances, reputation and intellectual property. If the organisation provides critical aviation services then the results of the national risk assessment should be taken into account. The risk management process must explicitly set out its scope i.e. state which risks it will address and what the treatment is of those that are in scope.

⁸ "Likelihood" is expressed as "Level of Trust" in ED-202A and ED-203

⁹ By the European Civil Aviation Conference (ECAC) or other ICAO regional bodies.

¹⁰ The European Union has national responsibility for some aspects of aviation safety and security.

¹¹ At the international level, ICAO's Aviation Security Handbook (Doc 8973) Chapter 9 also discusses risk management in the context of an organisation's Security Management System (SeMS).

2.4.2

Risk Management Methods

Although the basic principles of risk management are well established and widely agreed the practicalities of applying risk management in general (and risk assessment in particular) mean that numerous different methodologies have been developed to fit particular circumstances and environments. This applies to both overall security risk and to particular topics such as information security.

In information security in the context of this document, it is worth noting that there are different methodologies in use, such as:

- The ICAO Risk Context Statement (RCS) method is used by the ICAO Aviation Security Panel's Working Group on Threat and Risk to assess broad global risk issues at the international and national levels;
- ISO 27005 is the Information Security Risk Management standard from the International Standards Organisation, and is widely used by organisations as a framework for information risk management. It is part of a broader set of standards and guidance, which include control measures for risk reduction. Organisations which follow the 27000 approach can have their Information Security Risk Management System certified by independent auditors;
- The US National Institute of Standards and Technology (NIST) publishes a range of Special Publications on information security, including some which cover risk management and risk assessment. It is designed for US Federal Agencies, but is also applicable to other organisations. In particular SP800-39 provides guidance on an integrated, organisation-wide program for managing information security risk. SP 800-30¹² provides guidance for conducting risk assessments, amplifying the guidance in SP 800-39;
- ED-202A describes an Airworthiness Security Process for aircraft design which includes security risk management activities. These interact with the safety assessment process described in ED-79A/ARP4754A.

The RCS is an appropriate method at the international and national levels, and for considering broad threat issues. ISO27005 is designed as an organisational method, which can apply to all or part of an organisation's IT and control systems. The NIST methodology is also based on an organisational view and is designed for government organisations.

It is also worth considering how the ICAO Aviation Security Manual (Doc 8973) discusses what it describes as the "total risk landscape"¹³ as a way of describing how risks in different areas of civil aviation can be linked together or can affect each other. It recommends an integrated approach that considers risk targets and objectives across different areas to get greater risk coherence, and goes on to say:

"When risks are reduced in one area, new risks may arise elsewhere in the system, usually at the boundary with another system, at the boundary between two layers within the same system, or in areas of the system not formerly associated with significant risk. For example, the reduction of security-related risks in the flight operations area could lead to a migration of risk to the airport, reflecting a failure to achieve an overall reduction in risk. This is why management should consider the total risk "landscape", comprised of the system, its various internal layers and its boundaries with other systems, when evaluating the possible impact of different risk reduction approaches. As another example, a closed airport could compel aircraft to divert to another airport, thus exporting risk to the other airport and also to transport links with these facilities. In such a case, management should periodically evaluate risk across the entire transport sector, and not only separate elements of the sector in isolation.

¹² Guide for Conducting Risk Assessments, Rev. 1, Sep 2012

¹³ In Chapter 9.2

Risk targets and objectives evolve along with the sector itself, and thus are products of a sector-centric approach. A security risk management cycle works well, but remains comparatively inward looking. The alternative is to have a more integrated approach that considers risk targets and objectives from all areas involved and across different areas, leading to greater risk coherence.

In practice this requires three things:

- a. A wider-scope risk assessment to show the bordering interactions and impacts;*
- b. Comparative risk assessments across all areas involved; and*
- c. A total 'risk picture' that highlights the risk priorities."*

Thus to fully understand its own security position, each organisation will need to have an understanding of the security position of the organisations it co-operates with (i.e. its partners). As well as any commercial and regulatory requirements, making network connections and exchanging data is based on a trust assessment between the partners because trust is the reflection of the risks involved. The degree of trust determines the extent to which the network connections, network traffic and data needs to be controlled and checked.

To enable a secure interface/product the organisation must assess the trust it can place in the connection and/or in the data being received or the product. It must also be able to assure itself that the assessment is validated and remains valid over time. It is important to stress that this does not mean that an organisation needs to reveal everything about its security to its partners. What is needed is enough information to provide the required level of assurance based on risk assessments. The risk information needs to be shared to a level of detail which fits the levels of risk mutually agreed by the partners.

2.4.3

Acceptable Risk Levels

In some cases the relevant authority will have specified risk acceptability criteria, to show how risks will be deemed acceptable. In other cases it will need to be agreed between partners on a case by case basis such as between the applicant for a certification and the relevant authority. Between unregulated partners the acceptable risk level will need to be agreed and specified within an external agreement, as specified in 3.5.

In Civil Aviation many transnational aspects have been regulated through ICAO treaties (in the form of annexes to the ICAO Convention (Doc 7300)). As an example in Annex 8 the definition of "Anticipated operating condition" states that "*Anticipated operating conditions do not include: ...b) those extremes which occur so infrequently that to require the Standards to be met in such extremes would give a higher level of airworthiness than experience has shown to be necessary and practical*". Effectively this means, that a certain safety risk has been specifically accepted by all "contracting states". National Airworthiness Authorities have specified qualitative and quantitative probabilities of occurrence of Failure Conditions of certain severities. The highest level of severity, "catastrophic" shall be at least "extremely improbable", or occur less than 10^{-9} per flight hour (e.g. EASA CS-25 Book 2 AMC 25.1309 section 7). Again, an acceptable risk has been defined in terms of safety relevant events.

In contrast security is a collaborative effort between all stakeholders in aviation and thus needs a collaborative effort to coherently assess, comparably evaluate and concertedly accept risks. This includes a common understanding and agreement of the results of individual Risk Management approaches.

As there is currently no security-related regulation with respect to airworthiness certification, there are some aspects which are still undefined at the time of publication.